

**eZ-Audit**  
**Use-Case Specification 4: Maintain User Profile**

**Version 1.1**

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

## Revision History

Date	Version	Description	Author
7/17/2002	1.0	Final version created for 7/17 deliverable submission.	Matt Portolese
08/05/2002	1.1	Revised version created for deliverable re-submission	Matt Portolese

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

## Table of Contents

1.	Maintain User Profile	4
1.1	Brief Description	4
2.	Flow of Events	4
2.1	Basic Flow	4
2.2	Alternative Flows	5
2.2.1	User updates profile information and password.	5
2.2.2	Password in wrong format	5
2.2.3	Wrong old password	5
2.2.4	New password and re-typed new password did not match	6
2.2.5	Password same as one of previous 5 passwords	6
3.	Special Requirements	6
3.1	User will not be able to obtain current password once in the system.	6
4.	Preconditions	6
4.1	User accesses profile from their home page.	6
5.	Postconditions	7
5.1	User returns to home page.	7
6.	Extension Points	7
6.1	Use Case 1 “Manage Users”	7
6.2	Use Case 2 “View Submissions”	7
6.3	Use Case 15 “Select an Institution”	7
6.4	Use Case 13 “Assign Submissions”	7
7.	Validations	7
8.	Requirements	7

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

# Use-Case Specification 4: Maintain User Profile

## 1. Maintain User Profile

### 1.1 Brief Description

Any user will have the ability to update their personal profile, including changing their password in the eZ-Audit system. All users, internal and external will have access to the same profile information to maintain.

## 2. Flow of Events

### 2.1 Basic Flow

#### 1) General user actor selects “my profile” function from their home page.

The system retrieves the information from for the following fields and pre-populates them in the profile page:

- First Name
- Last Name
- Email address
- Office phone
- Office extension
- Fax

#### 2) System presents the “my profile” page.

The user is shown a page with the fields listed above and their information from the system prepopulated in text boxes. The system also presents three additional fields to be used for changing the password. The following text and field labels should be displayed:

“If you wish to change your password, please key in your old and new password in the spaces provided below. If no information is entered, your password will not change.

The password must be 8– 15 characters in length and must include at least 3 of the following types of characters: uppercase letters(A-Z), lowercase letters(a-z), numeral values(0-9) and special characters(<, >, ?, \$, etc.). The password must be dissimilar from your previous 5 passwords.”

Field labels with text boxes:

- Old password
- New password
- Re-type new password

Buttons:

- Save
- Reset

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

**3) The General User actor verifies that the profile information is correct and elects to change their password.**

The General User actor enters the old password, new password and re-types the new password into the appropriate fields. The user then presses the “Save button”

**4) The System displays the correct message.**

A pop-up box appears with the message:

“Your password has now been changed.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the home page.**

The appropriate home page is displayed.

## 2.2 Alternative Flows

### 2.2.1 User updates profile information and password.

Steps 1-2 are the same for the alternate use cases. Only the following steps will change.

**3) The General User actor verifies that the profile information is correct and elects to update their phone number.**

The General User actor deletes the existing phone number that is displayed and types in the new phone number. They also type in the old password, new password and re-types the new password into the appropriate fields. The user then presses the “Save button”

**4) The System displays the correct message.**

A pop-up box appears with the message:

“Your profile information and password has now been changed.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the home page.**

The appropriate home page is displayed.

### 2.2.2 Password in wrong format

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

**4) The System displays the correct message.**

A pop-up box appears with the message:

“The new password you entered does not meet system requirements. Passwords must be 8– 15 characters in length and must include at least 3 of the following types of characters: uppercase letters(A-Z), lowercase letters(a-z), numeral values(0-9) and special characters(<, >, ?, \$, etc.). The password must be dissimilar from your previous 5 passwords.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the profile page.**

The identification fields do not change (first name, last name, email, etc.). The old password, new password, and re-type new password fields have been set to blank.

### 2.2.3 Wrong old password

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

**4) The System displays the correct message.**

A pop-up box appears with the message:

“The old password you entered was incorrect, please try again.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the profile page.**

The identification fields do not change (first name, last name, email, etc.). The old password, new password, and re-type new password fields have been set to blank.

**2.2.4 New password and re-typed new password did not match**

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

**4) The System displays the correct message.**

A pop-up box appears with the message:

“The new passwords you typed in do not match, please try again.”

**5) The General User clicks the “OK” button on the pop-up box.**

**6) The System returns the user to the profile page.**

The identification fields do not change (first name, last name, email, etc.). The old password, new password, and re-type new password fields have been set to blank.

**2.2.5 Password same as one of previous 5 passwords**

Steps 1-3 are the same for the alternate use cases. Only the following steps will change.

**7) The System displays the correct message.**

A pop-up box appears with the message:

“Your password must be different than your previous five passwords. Please try again.

**8) The General User clicks the “OK” button on the pop-up box.**

**9) The System returns the user to the profile page.**

The identification fields do not change (first name, last name, email, etc.). The old password, new password, and re-type new password fields have been set to blank.

### **3. Special Requirements**

**3.1 User will not be able to obtain current password once in the system.**

Using LDAP, passwords are encrypted one way and are not able to be decrypted and read once in the system. Passwords can be compared, but not retrieved. If a user forgets his or her password, they will have to have their passwords reset by an administrator. See extension point – Use Case 1 “Manager Users”.

### **4. Preconditions**

**4.1 User accesses profile from their home page.**

A user will only be able to update their profile information.

- See extension point – Use Case 2 “View Submissions” for information on the external user home page.

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

- See extension point – Use Case 15 “Select an Institution” for information on the resolution user home page.
- See extension point – Use Case 13 “Assign Submissions” for information on the co-team leader user home page.

## 5. Postconditions

### 5.1 User returns to home page.

User will return to their home page once completed making profile changes.

- See extension point – Use Case 2 “View Submissions” for information on the external user home page.
- See extension point – Use Case 15 “Select an Institution” for information on the resolution user home page.
- See extension point – Use Case 13 “Assign Submissions” for information on the co-team leader user home page.

## 6. Extension Points

### 6.1 Use Case 1 “Manage Users”

Describes the steps needed to reset a user’s password.

### 6.2 Use Case 2 “View Submissions”

Describes the home page of the external user.

### 6.3 Use Case 15 “Select an Institution”

Describes the home page of the resolution user.

### 6.4 Use Case 13 “Assign Submissions”

Describes the home page of the co-team leader.

## 7. Validations

- First Name: Alpha; max 20
- Last Name: Alpha; max 30
- Email address: Alphanumeric and @ symbol; format: yourname@school.edu; max 50
- Phone and Fax number: Numeric; format 999-999-9999; max 10
- Password: At least 3 of each: Uppercase alpha, lowercase alpha, numeral values, and special characters(<, >, ?, \$, etc.); minimum 8 characters; maximum 15 characters; dissimilar from previous 5 passwords

## 8. Requirements

- GEN18 The system will support syntax rules that allow the following elements to be incorporated into passwords:· Alphanumeric values· Alpha-only values· Numeric-only values
- GEN19 The system will support rules that enforce the following capabilities:· Password lifetime from 120 days (ED User)· Unlimited password lifetime (Institution & Audit)· Comparison to 5 previous passwords for the user· Disabling of the account after a period of inactivity of 90 to 365 days
- GEN20 The system will support ED password syntax rules and management rules.
- GEN21 The system will support a minimum password length of 8 characters.
- GEN22 The system will support syntax rules that enforce at least three of the following conditions on

eZ-Audit	Version: 1.1
Use-Case Specification 4: Maintain User Profile	Date: 08/05/2002
Use Case 4	

every password:· Uppercase alphabetic characters (A-Z)· Lowercase alphabetic characters (a-z)· Numeral values (0-9)· Non-alphabetic and non-numeric characters ( < ! @ # etc.)

- GEN23 The system will support rules that enforce the following capabilities:· Password expires on the first logon attempt for a new user· Password uniqueness set to 5 - i.e., systems stores and recalls past 5 passwords· Automatic account lockout after 3 unsuccessful login attempts· Set Account Lockout button· Automatic log-out duration set to 30 minutes of inactivity - validate with session management req· Unsuccessful login counter reset to 0 from 3 after 30 minutes
- GEN24 The system will store passwords in an encrypted state in the credential repository.
- GEN70 The system will require passwords to adhere to FSA password syntax rule.
- GEN100 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her name on the Admin Profile page.
- GEN101 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her Email address on the Admin Profile page.
- GEN102 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her phone number on the Admin Profile page.
- GEN103 The system will provide each Ed user (Audit Resolution Specialist, Financial Analyst and Co-Team leader) with ability to update his/her fax number on the Admin Profile page.